UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/750,255	12/28/2000	Theodore Jack London Shrader	AUS920000851US1	7414

7590 07/28/2009

Darcell Walker
8107 Carvel Lane
Houston, TX 77036

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte THEODORE JACK LONDON SHRADER,
RANDY SCOTT HUMPHREY,
DAVIS KENT SOPER,
and XIAOYAN ZHANG

Appeal 2007-003855
Application 09/750,255[1]
Technology Center 2100

Decided:[2] July 28, 2009

Before LEE E. BARRETT, LANCE LEONARD BARRY, and HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

BARRETT, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] Filed December 28, 2000, titled "Architecture for a Unified Synchronous and Asynchronous Sealed Transaction."

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

This is a decision on appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1-18. We have jurisdiction pursuant to 35 U.S.C. § 6(b).

We affirm.

STATEMENT OF THE CASE

The invention

The disclosed invention is directed to a communications method that enables secure transmission across multiple synchronous or asynchronous protocols and enables the recipient of a message to trace all of the events during the message's transmission.

The Background of the Invention discloses:

> Previous communication protocols have focused on transmission of a sealed transaction between two entities. In a typical SSL [Secure Sockets Layer] transaction such as sending a facsimile message, the destination can perform processing on the information and determine its origin and maintain the originality of the message. The recipient will know what entities were involved in the transaction along the transmission, the actual sender of the message, check to verify that each entity was able to sign that information confirming that they were able to take care of the information. An example is purchasing an item over the Internet. This type of transaction is an SSL transaction. However, sending an electronic mail message is an asynchronous transaction. With the expanded use of the Internet and other computing networks, there is a need to be able to have the ability to trace events in the transmission of the message regardless of whether the transmission is synchronous or asynchronous.

Spec. 4-5.

In the disclosed invention, the original transaction is packaged within a Public Key Cryptology Standard (PKCS) SignedData object, which is a

digitally-signed container for arbitrary message content. A SignedData object includes signed attributes consisting of the content or data type of the message, a message digest, and signing time. Recipients of a SignedData object can verify the message and signature using the sender's public key to ensure the authenticity of the sender and the integrity of the message. If the message has to be forwarded, the sender adds a new SignedData object, possibly with new information, including a message digest of the old message, known as a related message digest. Since message digest values are unique to the message for which the digest was generated, the related message digest attribute value allows the final or interim recipients to link the messages together to form the original chain of messages and determine the initial sender. Spec. 10-11.

In an asynchronous protocol, the SignedData or multiple SignedData objects are wrapped in an EnvelopedData object, which is an object that provides properties and methods to envelop data for privacy by encryption. Spec. 12.

The claims

Claim 1 is reproduced below:

1. A general communication transmission method that enables a transmitted message to span synchronous and asynchronous protocols over a computer network during one transmission comprising:

packaging a message for transmission in a data object, the message packages including information on the original message in the transmission;

sending the packaged message to a designated recipient entity;

receiving the message by a current recipient entity at a location;

recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message; and

determining whether current recipient entity is the designated recipient entity.

The references

Sudia US 6,209,091 B1 Mar. 27, 2001
(filed Sep. 29, 1998)

Preston Gralla, *How the Internet Works* (4th ed. Que 1998), page 19, item 4.

Doug Lowe, *Internet Explorer 3 for Windows for Dummies* (IDG Books 1996), pages 139-153 ("*Internet Explorer for Dummies*").

Definition of "audit trail": "A record of business transactions that can be used by an interested party to trace an organization's activities to original documents. Audit trails are used to verify account balances." David L. Scott, *Wall Street Words: An A to Z Guide to Investment Terms* (Houghton Mifflin 2003), on http://dictionary.reference.com/.

The rejections

Claims 1-18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Sudia.

Claims 1 and 10 stand additionally rejected under 35 U.S.C. § 102(b) as being anticipated by *Internet Explorer for Dummies*.

Representative claim 1

Appellants argue the limitation of recording a "message transmission history" contained the "event" of a stop which is found in all independent claims in one form or another. Appellants do not argue the separate patentability of the claims. Thus, claim 1 is selected as representative. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2006).

PRINCIPLES OF LAW

Claim interpretation

During patent examination, when claims can be amended, claims are given their broadest reasonable interpretation. *In re Zletz*, 893 F.2d 319, 321-22 (Fed. Cir. 1989).

Anticipation

"Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983).

Arguments not made are waived

Arguments not made are considered waived. *See In re Baxter Travenol Labs.*, 952 F.2d 388, 391 (Fed. Cir. 1991) ("It is not the function of this court to examine the claims in greater detail than argued by an appellant, looking for nonobvious distinctions over the prior art."); *In re Wiechert*, 370 F.2d 927, 936 (CCPA 1967) ("This court has uniformly followed the sound rule that an issue raised below which is not argued in this court, even if it has been properly brought here by a reason of appeal, is regarded as abandoned and will not be considered. It is our function as a court to decide disputed issues, not to create them."); *In re Wiseman*, 596 F.2d 1019, 1022 (CCPA 1979) (arguments must first be presented to the Board before they can be argued on appeal).

DISCUSSION

Anticipation over Sudia

Issue

Have Appellants shown that the Examiner erred in finding that Sudia teaches "recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message" as recited in representative claim 1?

Contentions

The Examiner finds that Sudia teaches "recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message," as recited in

claim 1, "where the message transmission history is indicated by each of the parties that signed the document as it passes through the network. (Column 16, lines 45-52) & (Column 16, lines 57-65) & Figure 10." Final Off. Action 4; Ans. 5.

Appellants argue that the present invention distinguishes from Sudia in that: (1) the present invention is not supplying part of a predetermined signature to the message; (2) in the present invention, a modification or addition to the message can happen but may not happen, whereas in Sudia the purpose of the stop is to add another piece of the signature; and (3) in the present invention there is no predetermined set of stops. Supp. Br. 5.

Appellants argue:

> Sudia does not provide the capability to generate a history of the transmission path. The locations cited in Sudia (Column 16, lines 45-52 and 57-65 and Figure [10)] do not describe the [sic] recording the event of receiving the package message by a current recipient in a message transmission history generated for the transmitted message step of [sic] claimed in Applicants' present invention.

Supp. Br. 5.

The Examiner responds:

> The Examiner contends that because Sudia explicitly stated that the signatures as the document passes through the nodes are left "as an audit trail" (Column 16, line 63), the series of signatures may be considered a "transmission history". An audit trail is commonly understood as such: (taken from www.dictionary.com)
> audit trail

> A record of business transactions that can be used by an interested party to trace an organization's activities to original documents. Audit trails are used to verify account balances.
>
> Source: Wall Street Words: An A to Z Guide to Investment Terms for Today's Investor by David L. Scott. Copyright © 2003 by Houghton Mifflin Company. Published by Houghton Mifflin Company.

Ans. 11-12 (emphasis omitted).

Facts

Sudia describes that a Certification Authority (CA) for public key certificates affixes a signature key to sign certificates of high-value users and subordinate CAs, but the CA's signature key is a target for terrorists, criminals, and espionage. Col. 1, ll. 42-50.

Sudia describes a multi-step signing system and method that uses multiple signing devices to affix a single signature, which can be verified using a single public verification key. Each signing device possesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents. Abstract. In this way no single signing device needs to contain the signature key during the document signing operation and the system permits loss or compromise of one or more signing devices while maintaining available, un-compromised signing devices. Col. 2, ll. 25-39.

Sudia describes a multi-step signing example in connection with Figures 9 and 10. The end result is a document signed with a System Wide Authority (SWA) signature. The example assumes that two Authorizing

Agents 1a and 1b (human agents) authorize Signing Device 1 to affix a partial signature, and that Authorizing Agents 2a and 2b authorize Signing Device 2 to complete the SWA signature. Col. 16, ll. 21-32.

As shown best in Figure 9, Authorizing Agent 1a receives a request for a signature of an electronic message 131 having a header 133 and the document to be signed 135. Authorizing Agent 1a strips off the header, performs procedural checks, signs with the agent's secret signature key --AA1a, and sends the signed certificate to Authorizing Agent 1b. Authorizing Agent 1b strips off the header, performs procedural checks, signs with the agent's secret signature key --AA1b, and sends the twice-signed document 139 to Signing Device 1. Col. 16, ll. 33-65. "AA1*a*'s signature is left on the document as an audit trail." Col. 16, l. 63. The rejection finds that the step of attaching secret signature keys at the authorizing agent is "recording the event of receiving the package message" and the string of keys forms a "message transmission history."

Signing Device 1 verifies that the document has the necessary number of signatures and, if so, strips off the signatures of the authorizing agents, affixes a partial SWA signature, and sends the partially signed document 141 to an Authorizing Agent 2a for another signing device. The Authorizing Agents 2a and 2b affix secret signature keys in the manner previously described and send the signed document 149 to Signing Device 2 which completes the SWA signature. Col. 16, l. 66 to col. 17, l. 50.

Claim interpretation

Claim 1 is argued as representative. The preamble of claim 1 recites a "general communication transmission method that enables a transmitted message to span synchronous and asynchronous protocols over a computer network during one transmission." However, the body of the claim does not recite how synchronous and asynchronous protocols are treated differently. The Specification describes that synchronous protocols uses SignedData or multiple SignedData objects, while the asynchronous protocol uses SignedData or multiple SignedData objects wrapped in an EnvelopedData object (Spec. 10-12), which indicates that there is not a single method that handles both synchronous and asynchronous cases. The term "that enables" is a statement of capability that can mean that the method allows other, unclaimed, steps to perform the transmission as disclosed. In any case, the synchronous and asynchronous protocols limitation is not argued.

Claim 1 recites "packaging a message for transmission in a data object," but does not state any specifics of the packaging. At this point in the claim, "packaging" could be identifying a discrete message or packet.

Claim 1 recites "recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message," which is the only limitation at issue in this appeal. First, this limitation does not describe what "recording the event of receiving" or "a message transmission history" consist of. While the Specification discloses information such as a message digest, signing time, and a sender's private key (Spec.10), the claim is not so limited. The

"message transmission history" could be any information indicating who, where, or when the message was sent. Second, claim 1 next recites "determining whether current recipient entity is the designated recipient entity." It seems that the step of "recording the event of receiving . . . in a message transmission history" would only be performed if the "current recipient entity" is *not* "the designated recipient entity." However, claim 1 requires always "recording the event of receiving."

Analysis

It is clear that the Examiner is not saying that Sudia discloses Appellants' disclosed invention, but is rejecting the claims because they are so broadly drafted that they read on Sudia. Given our interpretation that claim 1 does not recite how synchronous and asynchronous protocols are treated differently, and that term "that enables" is a statement of capability that means the method allows other, unclaimed, steps to perform the transmission over synchronous and asynchronous protocols, it is not clear why the claims do not read on the SSL protocol described in the Specification at pages 4-5. As stated, "[t]he recipient will know what entities were involved in the transaction along the transmission, the actual sender of the message . . ." (Spec. 4, ll. 29-30), which indicates that the protocol provides a message transmission history.

Nevertheless, the rejection finds that the step of attaching secret signature keys at the authorizing agent is "recording the event of receiving the package message" and the string of keys form a "message transmission

history." As noted in the claim interpretation, the claims do not describe what "recording the event of receiving" or "a message transmission history" consists of. Thus, we agree with the Examiner that attaching an authorizing agent's secret signature key is "recording the event of receiving the package message." The signed message 139 from Authorizing Agent 1b to the Signing Device 1 contains both Authorizing Agent 1a's and Authorizing Agent 1b's secret signatures, --AA1a and --AA1b, which forms an "audit trail" (col. 16, l. 63), which is a "message transmission history," as broadly claimed. That is, the claims do not preclude a message transmission history from being a history of the persons who signed the document. The fact that the signatures are stripped off when the document is partially signed is irrelevant since a portion of the process in Sudia meets the limitation.

Appellants' arguments that the present invention distinguishes from Sudia in that the present invention is not supplying part of a predetermined signature to the message, is not necessarily modifying or adding to the message, and has no predetermined set of stops, are not persuasive because the arguments only argue what Sudia does that the invention does not and do not address why Sudia does not meet the claim language.

Appellants' argument that "Sudia does not provide the capability to generate a history of the transmission path" (Supp. Br. 5) is not persuasive because claim 1 recites a "message transmission history," not a history of the transmission path. The "history" can refer to a sequence of persons (such as the authorizing agents in Sudia), places, or times.

Therefore, Appellants have not shown error in the Examiner's finding of anticipation.

Conclusion

Appellants have not shown that the Examiner erred in finding that Sudia teaches "recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message" as recited in representative claim 1. Accordingly, the rejection of claims 1-18 is affirmed.

Anticipation over Internet Explorer for Dummies

Issue

Have Appellants shown that the Examiner erred in finding that *Internet Explorer for Dummies* teaches "recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message" as recited in representative claim 1?

Contentions

The Examiner finds that *Internet Explorer for Dummies* teaches "recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message," as recited in claim 1, at Figure 11-1, page 140. Final Off. Action 3; Ans. 4.

Appellants argue that this figure of *Internet Explorer for Dummies* shows a list of received e-mail messages and "does not describe the activity

of the message transmission history-generating step of Applicants present invention." Supp. Br. 6. It is argued that this figure of the reference "does not describe a method of implementing the present invention. Therefore, the reference does not provide an enabling description of Applicants' present invention." *Id.*

The Examiner responds that Figure 11-1 discloses e-mails received and "[w]ith each message or transmission, it can be determined who a message was sent from, along with the date and time of transmission and reception, along with a subject header to broadly summarize the subject matter of the message." Ans. 13.

Facts

Internet Explorer for Dummies shows a list of received e-mail messages, where each e-mail indicates who the e-mail is from, the subject line, and the date and time the e-mail was received.

Analysis

As noted in the claim interpretation section, claim 1 does not describe what "recording the event of receiving" or "a message transmission history" consist of. Thus, we see no error in the Examiner's finding that recording the date and time the e-mail was received is "recording the event of receiving the packaged message" and the information constitutes a "message transmission history."

Appellants argue that Figure 11-1 of *Internet Explorer for Dummies* "does not describe the activity of the message transmission history

generating step of Applicants present invention." Supp. Br. 6. It is argued that this figure of the reference "does not describe a method of implementing the present invention. Therefore, the reference does not provide an enabling description of Applicants' present invention." *Id.* Since Appellants merely deny that the limitation is not shown, without addressing why the date and time data is not a message transmission history, as broadly claimed, Appellants have not shown error in the Examiner's rejection. Appellants' argument that the reference does not provide an enabling description is not persuasive since the e-mail is a commercial product.

Conclusion

Appellants have not shown that the Examiner erred in finding that *Internet Explorer for Dummies* teaches "recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message" as recited in representative claim 1. Accordingly, the anticipation rejection of claims 1 and 10 is affirmed.

CONCLUSION

The rejection of claims 1-18 under 35 U.S.C. § 102(e) over Sudia is affirmed.

The rejection of claims 1 and 10 under 35 U.S.C. § 102(b) over *Internet Explorer for Dummies* is affirmed.

Requests for extensions of time are governed by 37 C.F.R. § 1.136(b).

See 37 C.F.R. § 41.50(f).

AFFIRMED

rwk

Darcell Walker
8107 Carvel Lane
Houston, TX 77036